Microsoft Security Response Center

Customer Guidance on Recent Nation-State Cyber Attacks

MSRC / By msrc / December 13, 2020

This post contains technical details about the methods of the actor we believe was involved in Recent Nation-State Cyber Attacks, with the goal to enable the broader security community to hunt for activity in their networks and contribute to a shared defense against this sophisticated threat actor.

As we wrote in that blog, while these elements aren't present in every attack, this is a summary of techniques that are part of the toolkit of this actor.

- An intrusion through malicious code in the SolarWinds Orion product. This results in the attacker gaining a foothold in the network, which the attacker can use to gain elevated credentials. Microsoft Defender now has detections for these files. Also, see SolarWinds Security Advisory.
- Once in the network, the intruder then uses the administrative permissions acquired through the on-premises compromise to gain access to the organization's global administrator account and/or trusted SAML token signing certificate. This enables the actor to forge SAML tokens that impersonate any of the organization's existing users and accounts, including highly privileged accounts.
- Anomalous logins using the SAML tokens created by the compromised token signing certificate can then be made against any on-premises resources (regardless of identity system or vendor) as well as to any cloud environment (regardless of vendor) because they have been configured to trust the certificate. Because the SAML tokens are signed with their own trusted certificate, the anomalies might be missed by the organization.
- Using the global administrator account and/or the trusted certificate to impersonate highly privileged accounts, the actor may add their own credentials to existing applications or service principals, enabling them to call APIs with the permission assigned to that application.

Due to the critical nature of this activity, Microsoft is sharing the following information to help detect, protect, and respond to this threat.

Activity Description

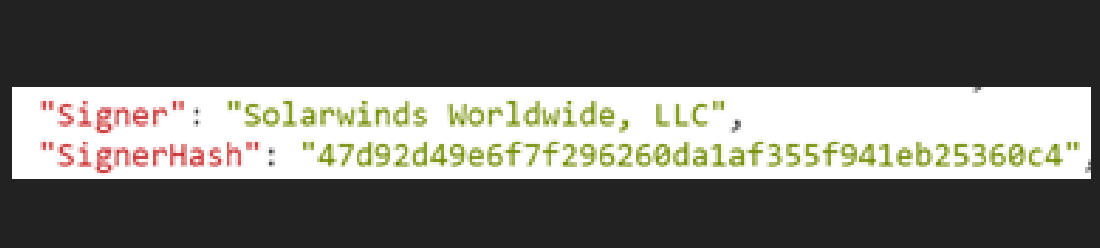
Initial Access

Although we do not know how the backdoor code made it into the library, from the recent campaigns, research indicates that the attackers might have compromised internal build or distribution systems of SolarWinds, embedding backdoor code into a legitimate SolarWinds library with the file name *`SolarWinds.Orion.Core.BusinessLayer.dll`*. This backdoor can be distributed via automatic update platforms or systems in target networks seen globally since March 2020. Microsoft security researchers have limited information about how they compromised the said platforms at this point.

Execution

While updating the SolarWinds application, the embedded backdoor code loads before the legitimate code executes. Organizations are misled into believing that no malicious activity has occurred and that the program or application dependent on the libraries is behaving as expected.

The attackers have compromised signed libraries that used the target companies' own digital certificates, attempting to evade application control technologies. Microsoft already removed these certificates from its trusted list. The certificate details with the signer hash are shown below:



```
"Signer": "Solarwinds Worldwide, LLC",
"SignerHash": "47d92d49e6f7f296260da1af355f941eb25360c4",
```

The DLL then loads from the installation folder of the SolarWinds application. Afterwards, the main implant installs as a Windows service and as a DLL file in the following path using afolder with different names:

- SolarWinds Orion installation folder, for example, `%PROGRAMFILES%\SolarWinds\Orion\SolarWinds.Orion.Core.BusinessLayer.dll`
- The .NET Assembly cache folder (when compiled) `%WINDIR%\System32\config\systemprofile\AppData\Local\assembly\tmp\<VARIES>\SolarWinds.Orion.Core.BusinessLayer.dll`

Microsoft security researchers observed malicious code from the attacker activated only when running under ***`SolarWinds.BusinessLayerHost.exe`*** process context for the DLL samples currently analyzed.

Command-and-control (C2)

The malicious DLL calls out to a remote network infrastructure using the domains *avsvmcloud.com*. to prepare possible second-stage payloads, move laterally in the organization, and compromise or exfiltrate data.

Microsoft detects the main implant and its other components as Solorigate.

Actions on Objectives

In actions observed at the Microsoft cloud, attackers have either gained administrative access using compromised privileged account credentials (e.g. stolen passwords) or by forging SAML tokens using compromised SAML token signing certificates.

In cases where we see SAML token signing certificate compromise, there are cases where the specific mechanism by which the actor gains access to the certificate has not been determined. In the cases we have determined that the SAML token signing certificate was compromised, common tools were used to access the database that supports the SAML federation server using administrative access and remote execution capabilities.

In other cases, service account credentials had been granted administrative privileges; and in others, administrative accounts may have been compromised by unrelated mechanisms. Typically, the certificate is stored on the server that provides the SAML federation capabilities; this makes it accessible to anyone with administrative rights on that server, either from storage or by reading memory.

Once the certificate has been acquired, the actor can forge SAML tokens with whatever claims and lifetime they choose, then sign it with the certificate that has been acquired. By doing this, they can access any resources configured to trust tokens signed with that SAML token signing certificate. This includes forging a token which claims to represent a highly privileged account in Azure AD.

As with on premises accounts, the actor may also gain administrative Azure AD privileges with compromised credentials. This is particularly likely if the account in question is not protected by multi-factor authentication.

Regardless of whether the actor minted SAML tokens or gained access to Azure AD through other means, specific malicious activities have been observed using these administrative privileges to include long term access and data access as described below.

Long Term Access

Having gained a significant foothold in the on premises environment, the actor has made modifications to Azure Active Directory settings to facilitate long term access.

1. Federation Trusts
   - Microsoft has observed the actor adding new federation trusts to an existing tenant or modifying the properties of an existing federation trust to accept tokens signed with actor-owned certificates.
2. OAuth Application & Service Principal Credentials
   - The actor has been observed adding credentials (x509 keys or password credentials) to one or more legitimate OAuth Applications or Service Principals, usually with existing *Mail.Read* or *Mail.ReadWrite* permissions, which grants the ability to read mail content from Exchange Online via Microsoft Graph or Outlook REST. Examples include mail archiving applications. Permissions are usually, but not always, AppOnly.
   - The actor may use their administrator privileges to grant additional permissions to the target Application or Service Principal (e.g. *Mail.Read*, *Mail.ReadWrite*).

Data Access

Data access has relied on leveraging minted SAML tokens to access user files/email or impersonating the Applications or Service Principals by authenticating and obtaining Access Tokens using credentials that were added in 2a. Above. The actor periodically connects from a server at a VPS provider to access specific users' emails using the permissions granted to the impersonated Application or Service Principal. In many cases, the targeted users are key IT and security personnel. By impersonating existing applications that use permissions like *Mail.Read* to call the same APIs leveraged by the actor, the access is hidden amongst normal traffic. For this reason, if you suspect you are impacted you should assume your communications are accessible to the actor.

Recommended Defenses

If your organization has not been attacked or compromised by this actor, Microsoft recommends you consider the following actions to protect against the techniques described above as part of your overall response. This is not an exhaustive list, and Microsoft may choose to update this list as new mitigations are determined:

1. Run up to date antivirus or EDR products that detect compromised SolarWinds libraries and potentially anomalous process behaviour by these binaries. Consider disabling SolarWinds in your environment entirely until you are confident that you have a trustworthy build free of injected code. For more details consult SolarWinds' Security Advisory.
2. Block known C2 endpoints listed below in IOCs using your network infrastructure.
3. Follow the best practices of your identity federation technology provider in securing your SAML token signing keys. Consider hardware security for your SAML token signing certificates if your identity federation technology provider supports it. Consult your identity federation technology provider for specifics. For Active Directory Federation Services, review Microsoft's recommendations here: Best Practices for Securing ADFS
4. Ensure that user accounts with administrative rights follow best practices, including use of privileged access workstations, JIT/JEA, and strong authentication. Reduce the number of users that are members of highly privileged Directory Roles, like Global Administrator, Application Administrator, and Cloud Application Administrator.
5. Ensure that service accounts and service principals with administrative rights use high entropy secrets, like certificates, stored securely. Monitor for changes to secrets used for service accounts and service principals as part of your security monitoring program. Monitor for anomalous use of service accounts. Monitor your sign ins . Microsoft Azure AD indicates session anomalies, as does Microsoft Cloud App Security if in use.
6. Reduce surface area by removing/disabling unused or unnecessary applications and service principals. Reduce permissions on active applications and service principals, especially application (AppOnly) permissions.
7. See Secure your Azure AD identity infrastructure for more recommendations.

Microsoft has published several detections to Azure Sentinel that provide additional signals for post-compromise techniques observed in these intrusions. For customers that do not have Azure Sentinel, the same detection logic can be used for hunting through the Unified Audit Log (UAL):

- Anomalous Azure Active Directory PowerShell behavior
- Modified domain federation trust settings
- New access credential added to OAuth Application or Service Principal

Microsoft Defender antivirus provides detections for threat components under the following detection:

Trojan:MSIL/Solorigate.B!dha

Detection version 1.329.368.0 or higher. If you believe your organization has been compromised, we recommend that you comprehensively audit your on premises and cloud infrastructure to include configuration, per-user and per-app settings, forwarding rules, and other changes the actor may have made to persist their access. In addition, we recommend comprehensively removing user and app access, reviewing configurations for each, and re-issuing new, strong credentials in accordance with documented industry best practices.

Indicators of Compromise (IOCs)

The below list provides IOCs observed during this activity. We encourage our customers to implement detections and protections to identify possible prior campaigns or prevent future campaigns against their systems. This list is not exhaustive and may expand as investigations continue. We also recommend your review the IOCs provided by FireEye at Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | FireEye Inc.

Command and Control

avsvmcloud[.]com	Command and Control (C2)

Observed malicious instances of SolarWinds.Orion.Core.BusinessLayer.dll

SHA256
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af

---

Analyst's comment: These indicators should not be considered exhaustive for this observed activity. Moreover, aside from the malicious DLLs, Microsoft researchers have observed two files in October 2019 with code anomalies when a class was added to the SolarWinds DLL. Note however that these two do not have active malicious code or methods.

Share

← Previous Post

Search …

Follow MSRC

Categories

BlueHat (178)
Japan Security Team (904)
MSRC (931)
Security Research & Defense (368)

Tags

advisory (60) ANS (47) Attack (43) Attack Vector (68) Black Hat (33) BlueHat Security Briefings (55) Community-based Defense (77) Defense-in-depth (38) EcoStrat (34) EMET (68) Exploitability (76) Internet Explorer (IE) (156) malware (59) Microsoft Office (81) Microsoft Windows (106) Mitigations (126) monthly bulletin release (48) rating (48) Risk Assesment (104) security (74) Security Advisory (134) Security Bulletin (133) security bulletin release (44) Security Bulletins (39) Security Conference Engagement (56) Security Ecosystem (52) Security Engineering (42) Security Research (72) Security Update (138) Security Update Webcast (46) Security Update Webcast Q & A (70) Update Tuesday (61) Webcast (37) Windows Update (68) Workarounds (74) Zero-Day Exploit (36) アドバイザリ (135) セキュリティ (53) セキュリティ情報 (430) セキュリティ更新 (66) ワンポイント (39) 啓発 (44) 展開 (45) 時事ネタ (42) 脆弱性 (226)

Recent Posts

Customer Guidance on Recent Nation-State Cyber Attacks
Security Update Guide: Let's keep the conversation going
Vulnerability Descriptions in the New Version of the Security Update Guide
Attacks exploiting Netlogon vulnerability (CVE-2020-1472)
Announcing the Top MSRC 2020 Q3 Security Researchers

Archives

Select Month

Copyright © 2020 Microsoft Security Response Center | Powered by MSRC Blog